NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COVERT HALF DUPLEX DATA LINK USING RADAR-EMBEDDED COMMUNICATIONS WITH VARIOUS MODULATION SCHEMES

by

Ehren J. Bittner

December 2017

Thesis Advisor:	Ric A. Romero
Second Reader:	Frank Kragh

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE 15 December 2017	3. REPORT TYPE AND DATES COVERED Master's Thesis 09-15-2015 to 12-15-2017

4. TITLE AND SUBTITLE COVERT HALF DUPLEX DATA LINK USING RADAR-EMBEDDED COMMUNICATIONS WITH VARIOUS MODULATION SCHEMES	5. FUNDING NUMBERS
6. AUTHOR(S) Ehren J. Bittner	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this document are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol Number: N/A.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

We consider the design of a low probability of intercept (LPI) half-duplex communications system in which the downlink is established via communications signals embedded in a pulsed-radar Doppler waveform. Previous works suggest to embed the communications in the radar backscatter where it has been shown possible to recover and demodulate communications signals that are coincident with the radar pulses in time and frequency using quadrature phase-shift keying (QPSK) modulation. Unfortunately, such an approach presents difficulty for a two-way link. In this work, we present a LPI half-duplex design where the downlink communications are embedded in the radar transmission, while the uplink may be transmitted via another covert method after the radar initiates communications. We illustrate the downlink using binary phase-shift keying (BPSK), QPSK, eight phase-shift keying (8PSK), quadrature-amplitude modulation (QAM), and explore a non-standard 8PSK for LPI. We show that probability of detection for the radar is actually improved by correlating to the radar-downlink signal. We also show that the downlink is feasible via symbol error rate (SER) results by estimating the radar signal parameters and subtracting the radar waveform from the received signal prior to demodulation. Further, we explore a qualitative analysis of this communications method to measure its covertness using the signal's complex plane.

14. SUBJECT TERMS communications, radar, interference, probability of detection, estimation, cancelation, low probability of intercept	15. NUMBER OF PAGES 65
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

THIS PAGE INTENTIONALLY LEFT BLANK

COVERT HALF DUPLEX DATA LINK USING RADAR-EMBEDDED COMMUNICATIONS WITH VARIOUS MODULATION SCHEMES

Ehren J. Bittner
Lieutenant Commander, United States Navy
B.ChE., University of Minnesota, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2017

Approved by: Ric A. Romero
Thesis Advisor

Frank Kragh
Second Reader

R. Clark Robertson
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

We consider the design of a low probability of intercept (LPI) half-duplex communications system in which the downlink is established via communications signals embedded in a pulsed-radar Doppler waveform. Previous works suggest to embed the communications in the radar backscatter where it has been shown possible to recover and demodulate communications signals that are coincident with the radar pulses in time and frequency using quadrature phase-shift keying (QPSK) modulation. Unfortunately, such an approach presents difficulty for a two-way link. In this work, we present a LPI half-duplex design where the downlink communications are embedded in the radar transmission, while the uplink may be transmitted via another covert method after the radar initiates communications. We illustrate the downlink using binary phase-shift keying (BPSK), QPSK, eight phase-shift keying (8PSK), quadrature-amplitude modulation (QAM), and explore a non-standard 8PSK for LPI. We show that probability of detection for the radar is actually improved by correlating to the radar-downlink signal. We also show that the downlink is feasible via symbol error rate (SER) results by estimating the radar signal parameters and subtracting the radar waveform from the received signal prior to demodulation. Further, we explore a qualitative analysis of this communications method to measure its covertness using the signal's complex plane.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

8PSK	eight phase-shift keying
AM	amplitude modulation
A/D	analog-to-digital
AIS	automatic identification system
AWGN	additive white Gaussian noise
BPSK	binary phase-shift keying
COLREGs	Convention on the International Regulations for Preventing Collisions at Sea
C-SNR	communications signal-to-noise ratio
CW	continuous wave
DPSK	differential phase-shift keying
DSP	digital signal processing
DSSS	direct sequence spread spectrum
DQPSK	differential quadrature phase-shift keying
EEMS	engineering enclave for maritime cyber security
FPGA	field programmable gate array
GPS	global positioning system
IMO	international maritime organization
I/Q	in-phase and quadrature
JTAG	Joint Test Action Group

LSE	least-squares error
LPI	low probability of intercept
MC	Monte Carlo
MLD	maximum-likelihood detector
NC-DQPSK	non-coherent differential quadrature phase-shift keying
PD	pulsed Doppler
PPI	plan position indicator
PRI	pulse-repetition interval
PSD	power spectral density
PSK	phase shift keying
QAM	quadrature-amplitude modulation
QPSK	quadrature phase shift keying
RCR	radar-to-communications ratio
RDM	range Doppler map
RF	radio frequency
SER	symbol error ratio
SNR	signal-to-noise ratio
SRBR	symbol rate-to-bandwidth ratio

Acknowledgments

I would like to thank my siblings and parents. Y'all have a way of both keeping me grounded, and motivating me to reach for the stars. Mom and Dad, you've instilled in me a love of lifelong learning and liberal education - that is a gift I will always cherish. I would not be here without your love and encouragement.

I would like to thank Jordan Cohen and Dr. Spencer Miller. Your support through this process has been tremendous. Thank you for blazing the trail, and for your guidance, and motivation.

I would like to acknowledge my thesis advisor, Dr. Romero. Thank you for all of your patience and help. Thank you for bringing me into this exciting field, and letting me be a part of some really cool work. You have been a great mentor.

Finally, I would like to thank my family. Mary, you have been my rock. I cannot express my undying gratitude for all that you do. You are a better partner than I deserve. Victor, Claire, and Tim - thank you guys for your understanding while Dad spent time studying and doing homework instead of playing with you. Your constant joy and enthusiasm have kept me energized. Your dad loves you, and misses you when he is at work.

Ad majorem Dei gloriam.

Laudetur Jesus Christus.
Nunc et in aeternum!

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1: Introduction

The world has used sea lanes of communications for centuries to move goods and ideas. According to the International Maritime Organization (IMO), we see that 90% of the world's trade takes place on the sea [1]. The large ships that transport these goods are required to maintain situational awareness through a variety of sensors, especially radar. Rule 5 of the Convention on the International Regulations for Preventing Collisions at Sea (COLREGs) requires ships to "maintain a proper look-out by ... all means" [2]. For ease of piecing together information from the data gathered, the radar is usually integrated into bridge displays.

As we move through the information age, due to our voracious appetite for information, pressures for communications capacity increase. The U.S. Navy and other entities use radio frequency (RF) bandwidth for sensing the environment as well as for communications. In this thesis, we explore a way to increase the communication capacity available by placing the communications signal co-channel with a radar. We propose to embed communications within bandwidth already allocated to the radar, possibly without decreasing radar performance.

In this thesis research, we continue the previous works [3], [4], [5], [6] conducted through the Engineering Enclave for Maritime Cyber Security (EEMS) laboratory to understand the maritime cyber environment. As such, it is appropriate to discuss the maritime cyber terrain.

1.1 Maritime Cyber Terrain

Planners, when building a route, attempt to select the best route by studying a map. When military planners want to cause an effect, they consider the maneuver space. The effects are easy to conceptualize for physical terrain (land, air, sea, space); however, to obtain understanding of cyber's virtual terrain is more difficult. The cyber realm, while tied to physical infrastructure, is arranged in data-link layers ranging from operating systems, devices, applications, to routing information. A truck driver is tied to the road, but a cyber effect is tied to the data layer that moves the traffic. The trucker can choose a different road, whereas the cyber effect can reshape the network. In order to gain understanding of the cyber terrain, we must examine where vulnerabilities lie. Once found, we can determine if these vulnerabilities can be mitigated. Within the maritime cyber terrain, ships float with multiple connected networks that create a large attack surface. The attack surface consists of the various ways these networks send and receive data: chart updates, automatic identification system (AIS), global positioning system (GPS), navigational radar, weapons control radar, and various other communications paths. When ships get underway and communicate, the attack surface is dominated by radio frequency (RF) equipment [7].

Internal to a ship are multiple networks. There is a voyage network for planning and executing the ship's transit, an engineering network to help administer and control the propulsion plant, and a communications network for sending and receiving orders, coordinating with other ships, and communicating to the outside world. There may be an entertainment network for providing recreation as its own network or this may be a subset of the communications network. Few people understand the intersection of these networks. We think of them as having some intersection, as displayed in Figure 1.1. Different shipboard networks are displayed with the shared infrastructure (routers, switches, cabling, servers, computers, communications paths) shown by the overlaps in the Venn diagram [7].

Companies are under economic pressure to minimize hardware while maximizing performance characteristics. With our ever increasing need for information, data throughput is a key performance characteristic. This pressure causes reuse of cyber infrastructure aboard ship as shown in Figure 1.2. Some of the reasons that increased communications capacity is needed are illustrated in Figure 1.2. These reasons include remote monitoring of engineering systems, real-time maritime traffic data, and other specialized data requirements. As [8] states, "sensors and onboard equipment help lower costs, and improve productivity." Clearly there are business pressures to increase connectivity within the ship.

With commercial pressures to aggregate data to support business planning and engineering troubleshooting, it is unsurprising that there are news stories [9], [10] discussing the possibility of subverting the maritime cyber terrain for nefarious purposes.

Understanding both the inter-ship and intra-ship topology is crucial to grasp the maritime cyber terrain. To illuminate one portion of this field, we choose radar systems as our focus.

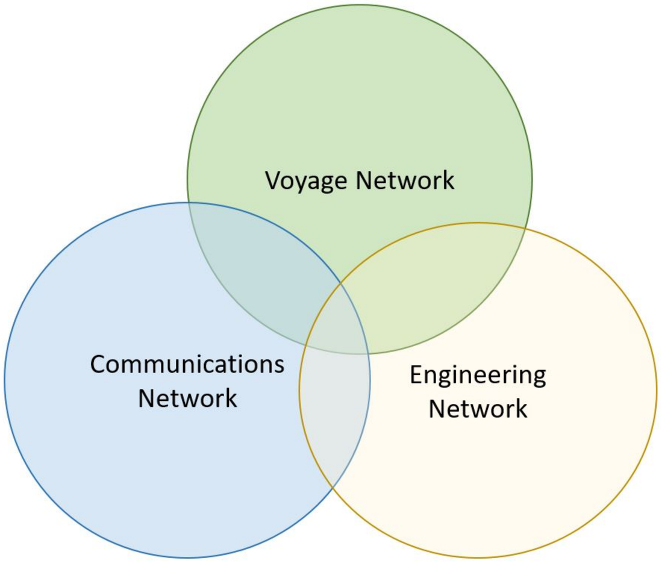

Figure 1.1. A Logical Layout of How Various Shipboard Networks Overlap. Adapted from [7].

Most ships are equipped with radar, and the radar is connected to the voyage network.

1.1.1 Embedded Communications

In order to meet the increasing demand for data throughput within the limits of the frequency spectrum already assigned, we propose to embed the communications signal within the radar pulse. Through embedding, we create a covert channel. This radar signal with embedded communications is the focus of this thesis work. The possible path for radar to affect the network, or to communicate, is illustrated in Figure 1.3. The steps necessary to take data embedded in RF energy to data bits traveling on a shipboard network are diagrammed in Figure 1.3. In this work, we explore the specifics of pulse detection, radar estimation and subtraction, and demodulation to discrete communications symbols.

Previous work has focused on embedding a communications signal in the backscatter of a radar pulse [3]–[6], [11], [12] in either a cooperative or non-cooperative manner. We now examine embedding and detecting communications symbols within the radar pulses from the actual radar emitter instead of the backscatter. The difference between this design and previous works is illustrated in Figure 1.4, where, in the left panel, previous works suggested to embed data link symbols onto the radar backscatter from STA-2. STA-1 then

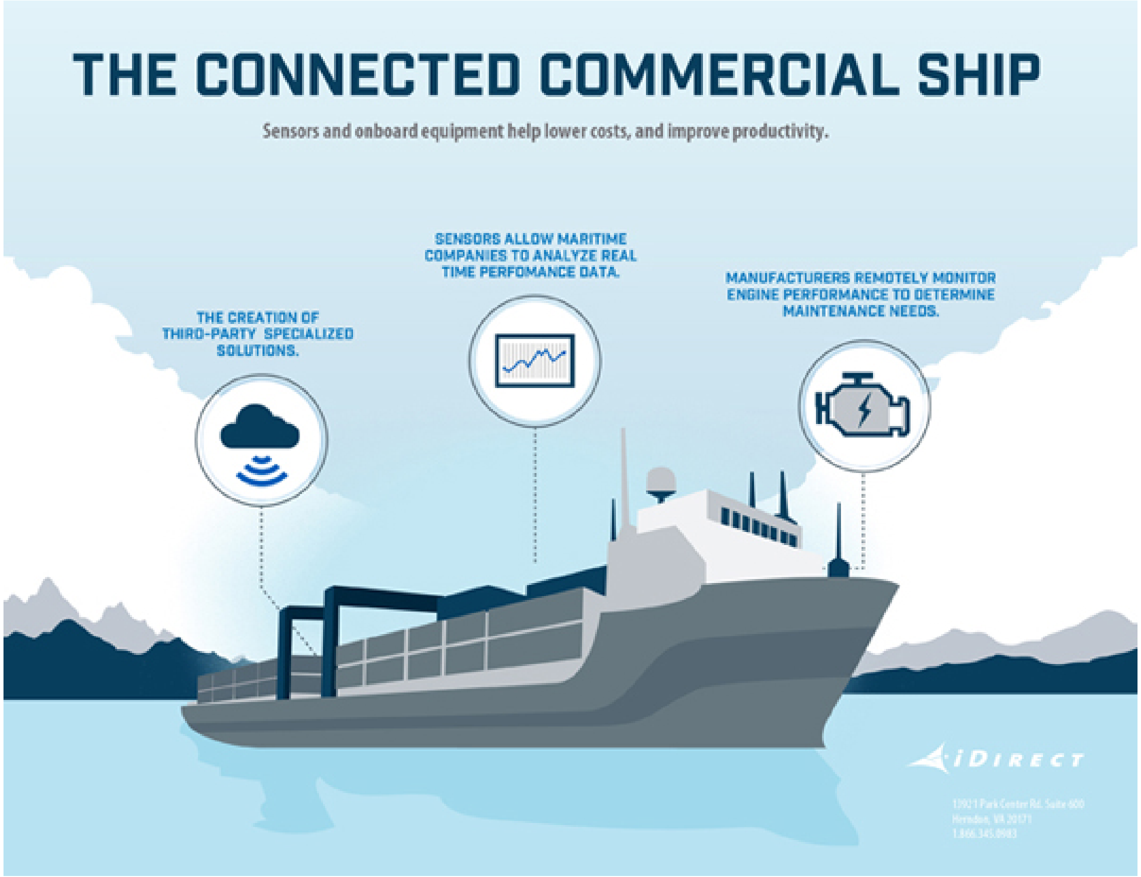
THE CONNECTED COMMERCIAL SHIP
Sensors and onboard equipment help lower costs, and improve productivity.
SENSORS ALLOW MARITIME COMPANIES TO ANALYZE REAL TIME PERFOMANCE DATA.
MANUFACTURERS REMOTELY MONITOR ENGINE PERFORMANCE TO DETERMINE MAINTENANCE NEEDS.
THE CREATION OF THIRD-PARTY SPECIALIZED SOLUTIONS.
iDIRECT
13921 Park Center Rd. Suite 600
Herndon, VA 20171
1.866.345.0983

Figure 1.2. A Graphic Developed for the Maritime Industry Displaying Their View of a Ship's Interconnected Networks. Source: [8].

demodulates the communications signal. On the right panel, the downlink of embedded symbols is implemented by the radar transmitter on STA-1 and uplink is established during the OFF time of the radar return using direct sequence spread spectrum (DSSS) from STA-2. In Figure 1.4, the radar signals and their returns are colored blue, while the DSSS signal is colored red. In the both panels, signals carrying communications are dashed lines and un-embedded signals are solid lines. No backscatter is shown in the right panel.

In the previous works mentioned, data transmission was limited to embedding within the radar backscatter and only provided one side of a communications link. There are some practical issues with this approach. Radar signal-to-noise ratio (SNR) is typically large to ensure both robust probability of detection and stringent probability of false alarm. In order to demodulate embedded communications, an increased SNR is required for further

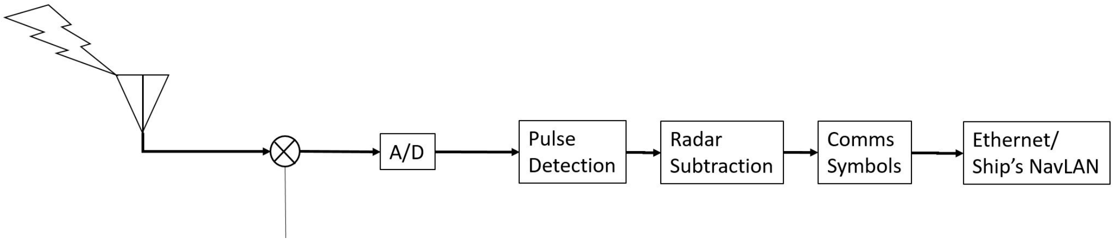

Figure 1.3. Flow Diagram Showing the Logical Steps Needed to Take a RF Signal and Convert it to Data Bits Traveling on the Maritime Network.

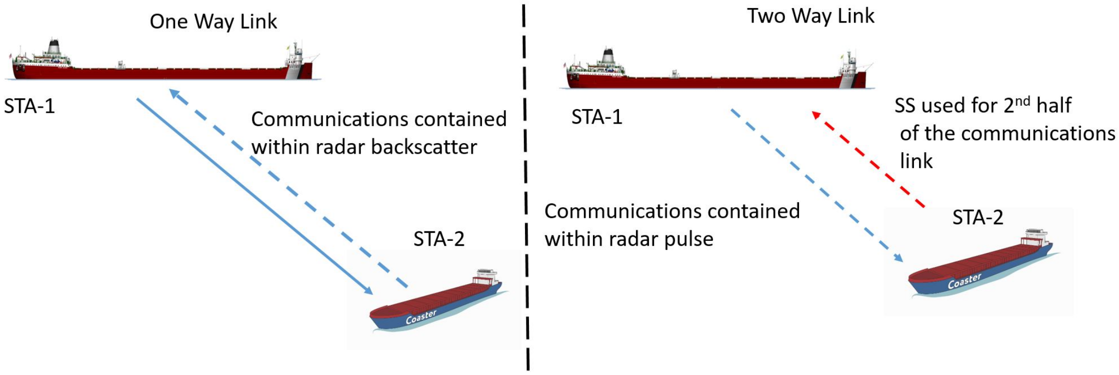
One Way Link
STA-1
Communications contained within radar backscatter
STA-2
Two Way Link
STA-1
SS used for 2nd half of the communications link
Communications contained within radar pulse
STA-2
Coaster
Coaster

Figure 1.4. Two Different Proposed Data Link Configurations Between Stations. Adapted from [5].

separation between the data symbols and noise to ensure meeting symbol error ratio (SER) requirements. Further, synchronizing the embedded data link symbols to the backscatter would be prohibitively difficult; both the hardware and software needed for radar estimation and coherent embedded synchronization would be extensive.

In this work, we investigate embedding the data link symbols within the radar pulses from the actual radar emitter instead of the backscatter. A benefit of this technique is that we can take advantage of the additional energy provided by the data symbols to potentially improve radar probability of detection (P_D) by correlating to the new radar-communications waveform instead of just the radar pulses. This would not have been possible with the backscatter case, as the radar would have no a priori knowledge of the embedded data.

While previous work focused on quadrature phase-shift keying (QPSK), differential phase-shift keying (DPSK), differential quadrature phase-shift keying (DQPSK), and non-coherent differential quadrature phase-shift keying (NC-DQPSK) [3]–[6], we expand the modulation schemes to include binary phase-shift keying (BPSK), eight phase-shift keying (8PSK), a modified 8PSK, and quadrature-amplitude modulation (QAM). Generally, throughout this thesis, we assume the communications signal's presence is obscured by its power in comparison to the significantly stronger radar signal instead of through other means. We use the radar-to-communications ratio (RCR) to describe the power of the radar signal relative to the embedded communications signal. We use the communications signal-to-noise ratio (C-SNR) to specify the power of the communications signal relative to the noise.

1.2 Covertness Evaluation

Previous work focused on evaluating radar-embedded communications impact to radar performance via plan position indicator (PPI) display [4]. We test our modulation schemes to determine their noticeability on a PPI. We analyze the covertness of the embedded signal by examining the phase plane (complex plane) of the received signal as seen by an eavesdropper on the STA-1 to STA-2 conversation. We assume that the eavesdropper is capable of the following: estimating the radar signal parameters, subtracting the radar from its received signal, and observing the phase plane of the residual signal. We assume that the non-cooperative eavesdropper is separately located from STA-2 and determine if it could detect the covert communications channel.

Previous work also examined at the effects on P_D with embedding in the backscatter [3]. The work in [4] found power spectral density (PSD) and range Doppler maps (RDM) are minimally impacted by backscatter embedding.

1.3 Objective

The discussion above motivates the investigation into establishing a half-duplex communications path. We explore two measures of performance. First, we measure the performance of the radar as a function of P_D. We test the P_D of match-filtered radar with and without embedded communications. Second, we explore the SER of the downlink to quantify the quality of the communications channel.

The proceeding sections also motivate an inquiry into the covertness of the embedded radar signal. We qualify covert communications through both the PPI display available to a radar operator and through the complex plane as viewed by an eavesdropper away from STA-2.

We conduct our investigation of the data-embedded radar channel in software using MATLAB and in hardware using Simulink and System Generator with a field programmable gate array (FPGA).

1.3.1 Thesis Organization

We organize the rest of the thesis in the following manner. In Chapter 2, we explore previous research in the area of co-channel radar and communications signals. We also present the mathematical models used for the radar and communications signals. The experimental methodology, detection, and demodulation techniques are discussed in Chapter 3. Results are presented in Chapter 4. Finally, conclusions and recommendations for future work are presented in Chapter 5.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Signal Models

In this chapter, we present the signal models necessary to mathematically represent radar, communications, and noise. We also discuss the various modulations used to embed the data into the radar waveform.

2.1 Signal Definitions

Adapted from previous works such as [3], [4] and [6], we assume a complex envelope signal model such that the signal transmitted from the radar antenna is $y(t) = r(t) + q(t)$ where $r(t)$ is the radar signal and $q(t)$ is the communications signal that "hides" within the radar pulse. Some amount of noise $w(t)$ is added within the receiver. We assume this noise is zero-mean additive white Gaussian noise (AWGN). Upon receipt and analog-to-digital (A/D) sampling, signal processing occurs. We use sufficiently high sampling rates to avoid aliasing. Additionally, we assume normalized sampling time where $T_S = 1$; therefore, the model of the received signal is

$$y[n] = r[n] + q[n] + w[n], \tag{2.1}$$

where the discrete-time sample index is $n = 0, 1, 2, \ldots.$ The radar can be either continuous wave (CW) or pulsed Doppler (PD). For this work, we concentrate on PD radars; thus, in the actual radar emission, we only embed the data symbols within the ON time of the pulse-repetition interval (PRI). The complex-valued radar baseband signal is given by

$$r[n] = \frac{A_r e^{j\phi_r}}{\sqrt{K}} \sum_{k=0}^{K-1} u_n[n - kT_r], \tag{2.2}$$

where A_r is the amplitude of the radar signal and ϕ_r is the phase of the radar pulse, which is assumed to be constant for the duration of that transmission. We note that in general, the phase may be different from pulse to pulse. That extension was previously addressed in [3]. The rectangular pulse train is represented by $\sum_{k=0}^{K-1} u_n[n - kT_r]$ and consists of K pulses where T_r is the PRI and $u_n[n]$ is given by

$$u_n[n] = \frac{1}{\sqrt{t_p}}(u[n] - u[n - t_p]), \tag{2.3}$$

where $u[n]$ is the unit step function and t_p is the time duration of the radar pulse. If $A_r = 1$, it follows that the pulse train described in Equation (2.2) is of unit energy; thus, A_r is the parameter we use to scale the radar signal energy for a particular radar SNR. The communications signal is modulated with either a modified PSK signal or a QAM signal. The modified phase-shift keying (PSK) signal has the same amplitude for each symbol; however, the QAM symbols are separated in both phase and amplitude. A mean magnitude $\overline{A}_q$ is defined as

$$\overline{A}_q = \frac{1}{M}\sum_{i=0}^{M-1} |A_q(i)|, \tag{2.4}$$

where $M = 16$ for 16QAM. The amplitude of the communications symbols is set by the power ratio of the radar signal and embedded communications signal, defined as the radar-to-communications ratio, or $RCR = {}^{P_r}/_{P_q}$. The power of the radar and communications signals are denoted by P_r and P_q, respectively. Since the communications signal is only present when the radar pulses are on, the RCR simply becomes an energy ratio:

$$RCR = \frac{A_r^2}{\overline{A}_q^2}. \tag{2.5}$$

If $\overline{A}_q = 1$, then the waveform described by Equation (2.4) is of unit energy; thus, A_q serves to scale the energy desired for this communications signal. It was shown in previous work that RCR does not affect SER significantly. Nevertheless, since our assumption is large RCR, we set RCR_{dB} to 20 dB in some portions of this work and for our Monte Carlo simulations.

We need a measure for how many communications symbols we attach to a given radar pulse. Following the convention established by [4], we choose the symbol rate-to-bandwidth ratio (SRBR). We define the symbol rate R_S as the reciprocal of the symbol duration T_s. Per convention we define the radar's bandwidth to be $B_r = {}^{1}/_{t_p}$ [13]; thus, our expression for

SRBR becomes

$$SRBR = \frac{R_S}{B_r}. \tag{2.6}$$

We vary SRBR between 1, 4, and 32 symbols per pulse in this work. The symbols are modulated as discussed in Section 2.2.

While not directly studied in this work, the act of embedding a communications signal into the radar pulse potentially improves the radar's range resolution ΔR [13] given by

$$\Delta R = \frac{ct_p}{2} = \frac{c}{2B_r}. \tag{2.7}$$

In other words, if the R_S is large, then the improvement in range resolution is given by

$$\Delta \hat{R} = \frac{c}{2R_S}. \tag{2.8}$$

A by-product of enlarging the symbol rate is a possible range resolution improvement for the radar.

2.2 Communications Signals

In this section, the methods for selecting a communications symbol and constructing the communications signal are discussed. We start with basic signals, then add complexity through the different modulation schemes.

The communications signal $q[n]$ is defined for the PSK modulations as

$$q[n] = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} A_q[k] e^{j\phi_q[k]} u_c[n - kT_r], \tag{2.9}$$

where $\phi_q[k]$ is the phase of the communications symbol, $A_q[k]$ is the amplitude of the communications symbol, and $u_c[n]$ is defined the same as $u_n[n]$ in Equation (2.3). In this equation, there is one symbol per pulse, but multiple symbols are easily accommodated in our simulations. If $A_q = 1$, then the signal described by Equation (2.9) is of unit energy; thus, we can use A_q to set the energy for the communications signal.

2.2.1 BPSK

For the BPSK signal, the symbols are a random draw from the set $\phi_q \in \left\{\pi, 2\pi\right\}$. As is true for all phase-shift keying symbols, data is encoded by the change in phase.

2.2.2 QPSK

For the QPSK signal, the symbols are again randomly drawn from the set $\phi_q \in \left\{\pi/4, 3\pi/4, 5\pi/4, 7\pi/4\right\}$. With the inclusion of two additional phase changes over BPSK, the amount of bits sent per symbol is twice that of BPSK.

2.2.3 8PSK

For the 8PSK signal, the symbols are a random draw from the set $\phi_q \in \left\{\pi/4, 2\pi/4, 3\pi/4, 4\pi/4, 5\pi/4, 6\pi/4, 7\pi/4, 8\pi/4\right\}$. The increase to eight phases increases the bit rate to three times that of BPSK.

2.2.4 Modified 8PSK

For the modified 8PSK signal, the symbols are a random draw from the set $\phi_q \in \left\{7\pi/36, 11\pi/36, 25\pi/36, 29\pi/36, 43\pi/36, 47\pi/36, 61\pi/36, 65\pi/36\right\}$. The phase map for this odd modulation is visualized in Figure 2.1. The blue circles represent each of the eight symbols in Figure 2.1, while the noise corrupted symbols appear as open orange circles. As with the unmodified 8PSK, three bits of information are sent with each symbol. The received signal constellation can be easily mistaken for QPSK, granting it a low probability of intercept (LPI) quality.

2.2.5 QAM

The previous work of [3]–[6], concentrated on PSK modulation schemes. We now extend the research to include forms of amplitude modulation (AM). The symbols for the standard 16QAM are a random draw from the set $\left\{-3-3j, -3-j, -3+j, -3+3j, -1-3j, -1-j, -1+j, -1+3j, 3-3j, 3-j, 3+j, 3+3j, 1-3j, 1-j, 1+j, 1+3j\right\}$. Notice that we can normalize the average energy of all the 16 possible constellation symbols; thus, we can easily arrive at the desired energy (when setting the SNR in our simulations) by using the average magnitude in Equation (2.4) to form the desired energy. With a choice of 16 possible values for each symbol, four bits of data can be sent with each symbol.

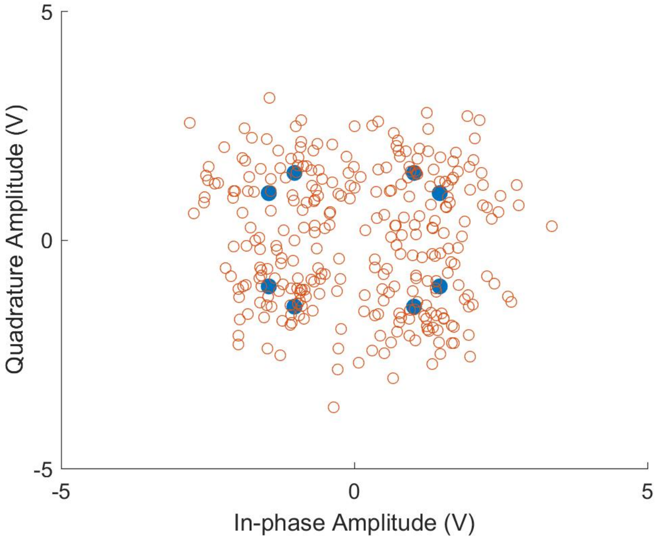

Figure 2.1. Phase Constellation for Modified 8PSK with Noise (SNR=5 dB).

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3: Detection and Demodulation Techniques

In order to sense the environment, we must detect and interpret radar-return pulses. The P_D for a radar is a function of the SNR and the probability of false alarm (PFA). Similarly for communications, the symbol transmitted must be demodulated by the receiver. In this chapter, we first explore the detection of the radar pulse. We then examine constructing and using an estimator of the radar signal such that we can recover the communications signal $q[n]$. Next we examine the demodulation of the residual communications signal. Finally, we examine the covertness of the combined radar/communications signal $y[n]$ using the PPI radar display and the complex plane of $y[n]$.

3.1 Radar Detection

In order for STA-2, the receiver as displayed in Figure 1.4, to recognize that STA-1 has sent data, it must detect the radar pulse. This classic detection problem is discussed in [14]. The problem is as follows:

$$\begin{aligned} H_0 &: x[n] = w[n] \\ H_1 &: x[n] = r[n] + w[n] \end{aligned} \tag{3.1}$$

for $n = 0, 1, ..., \hat{N} - 1$, where $\hat{N}$ is the number of samples. The null hypothesis (H_0) is the hypothesis that there is only noise present, while the alternate hypothesis (H_1) is that there is a signal present. To determine which choice to make, a test statistic is determined such that the PFA is met. For this work we used PFA = 0.001. We choose H_1 if $1/\hat{N} \sum_{n=0}^{\hat{N}-1} x[n]$ is greater than the threshold (γ). Following [14], we calculate γ as $\sqrt{\sigma^2\varepsilon/2}Q^{-1}(PFA)$, with σ^2 as the noise variance, ε as the signal energy, and $Q^{-1}(\bullet)$ is the inverse Q-function.

We can rearrange the equations for γ using our PFA to give the theoretical probability of detection

$$P_D = Q\left[Q^{-1}(PFA) - \sqrt{(\frac{2\varepsilon}{\sigma^2}^2)}\right]. \tag{3.2}$$

The Q-function is denoted by $Q(\bullet)$ [14].

3.2 Estimation

As discussed in [5], we use an estimator of various sizes N to estimate the magnitude and phase of the radar pulse $r[n]$ at STA-2's receiver. We let $r = A_r e^{j\phi_r}$ and $\underline{\mathbf{1}}$ is a column vector of N ones. Similarly, we let $\underline{\mathbf{q}} = \left[q[0], q[1], ..., q[N-1]\right]^T$ and $\underline{\mathbf{y}} = \left[y[0], y[1], ..., y[N-1]\right]^T$, where T indicates the transpose. The radar signal's least squares error (LSE) ($J(\hat{r})$) is of the form

$$J(\hat{r}) = \|\underline{\mathbf{y}} - (r\underline{\mathbf{1}} + \underline{\mathbf{q}})\|^2. \tag{3.3}$$

When the radar power is much greater than the communications power, Equation (3.3) can be approximated by

$$J(\hat{r}) \cong \|\underline{\mathbf{y}} - r\underline{\mathbf{1}}\|^2. \tag{3.4}$$

Then, the radar estimate ($\hat{r}$) is shown to be

$$\hat{r} = \frac{1}{N}\sum_{n=0}^{N-1} y[n]. \tag{3.5}$$

The magnitude estimate is found by taking the absolute value of Equation (3.5). The angle is found by taking the arctangent of the imaginary part of $\hat{r}$ divided by the real part of $\hat{r}$. One can see that the estimator improves as more terms are considered, i.e., by increasing N. Because N is critical to the estimate, we parameterize N in our Monte Carlo simulations to observe the effect of estimator size on SER. Once an estimate is determined, that estimate is subtracted from the received signal and is given by

$$\underline{\hat{\mathbf{q}}} = \underline{\mathbf{y}} - \hat{r}\underline{\mathbf{1}}. \tag{3.6}$$

The vector $\underline{\hat{\mathbf{q}}}$ is then demodulated through a maximum-likelihood detector (MLD) to determine the received data signal. Because 16QAM, 8PSK, and the modified 8PSK are more closely spaced than QPSK, larger estimator sizes than that utilized in [3] are used to produce better SER results. We employed $N \in \{0, 8, 16, 32, 64, 128, \text{full signal length}\}$ in this research. The case of $N = 0$ simply means that no estimator is used. For $N =$ full signal length, every discrete signal value is included in the estimator. In the succeeding results, full signal length varies from 300 to 30,000. As N increases, so does the signal processing time. In other words, for real-time applications N has to be a practical number. For real-time or near real-time communications, N needs to be chosen for an acceptable SER versus the processing delay.

3.3 Communications Demodulation

After detection and estimation, the communications signal undergoes demodulation. We use a MLD consisting of a bank of filters matched for each symbol to attempt to determine the correct symbol sent. We implement the MLD based on the a priori knowledge of the modulation scheme under test. The filter returning the highest value is chosen as the symbol; i.e., if filter R_1 (corresponding to symbol 1) returns the highest value, then symbol 1 is chosen.

We set the simulations such that the receiver does not know a priori the power, phase, or duration of the signal. We do this to test the end-to-end capability of the system, i.e, from pulse detection to demodulation.

3.4 Hardware Implementation of Detection and Demodulation

It has been shown previously that a FPGA achieves comparable SER results to that of the mathematical model [5] when applied to continuous wave radars. We now include FPGA detection of the radar pulse to the demodulation of the communications signal. Programming the FPGA was conducted graphically using the Xilinx blockset inside MATLAB's SIMULINK environment. The logical flow for hardware implementation is depicted in Figure 3.1.

The Xilinx Kintex 7 FPGA board used in this research is pictured in Figure 3.2. The FPGA has both an Ethernet and Joint Test Action Group (JTAG) connection to interface with MATLAB's Simulink environment. Both the hardware implementation and the Simulink model use the same input signal. This allows us to verify the Simulink model with hardware and test for any differences between software and hardware.

We conducted three co-simulations. All three used $N = 64$ with communications signal-to-noise ratio (C-SNR) of 10 dB and RCR of 20 dB. The correlation process and eventual

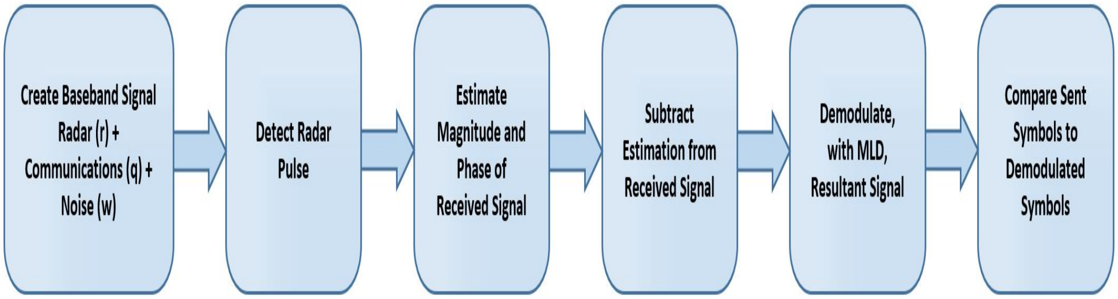
Create Baseband Signal Radar (r) + Communications (q) + Noise (w)
Detect Radar Pulse
Estimate Magnitude and Phase of Received Signal
Subtract Estimation from Received Signal
Demodulate, with MLD, Resultant Signal
Compare Sent Symbols to Demodulated Symbols

Figure 3.1. Creation, Detection, Estimation, Demodulation Procedure for FPGA Implementation. Adapted from [3].

detection were carried out through the use of matched filters as seen in Figure 3.3. The maximum of the output of the filters indicates the index $[n]$ that corresponds to the length of the signal. The output of the matched-filters can then be used to trigger the demodulation after estimation subtraction. We first demodulated a BPSK signal embedded in a pulsed-Doppler radar waveform. The model is shown in Figure 3.4. On the left of the model a BPSK signal generator constructs the BPSK-radar-noise signal that is passed to both the Simulink model and FPGA. The right most section contains the blocks demodulating the signals from the pure Simulink model and the FPGA ("BPSK Demodulator Baseband"). We compared these two bit streams to check for any differences in the results of the models. The second test is the detection and demodulation of a QPSK signal embedded in a pulsed-Doppler radar waveform. The model is visually represented in Figure 3.5. Following a layout similar to the BPSK case, the far left is the QPSK-radar signal generator. Demodulation and comparison occurs on the right portion of the model. The final co-simulation model tests the 16QAM embedded in a pulse Doppler radar waveform. The model is laid out as shown in Figure 3.6. The model maintains the same logical flow, signal generation is on the left, demodulation is on the far right, and estimation-subtraction is in the middle.

3.5 Communications Covertness

We now attempt different methods of qualifying the signal's covertness. We conducted this investigation through the use of the radar's visual display and the complex plane. For both parts of this section of the study, we fixed the RCR to 20 dB. This continues the assumption

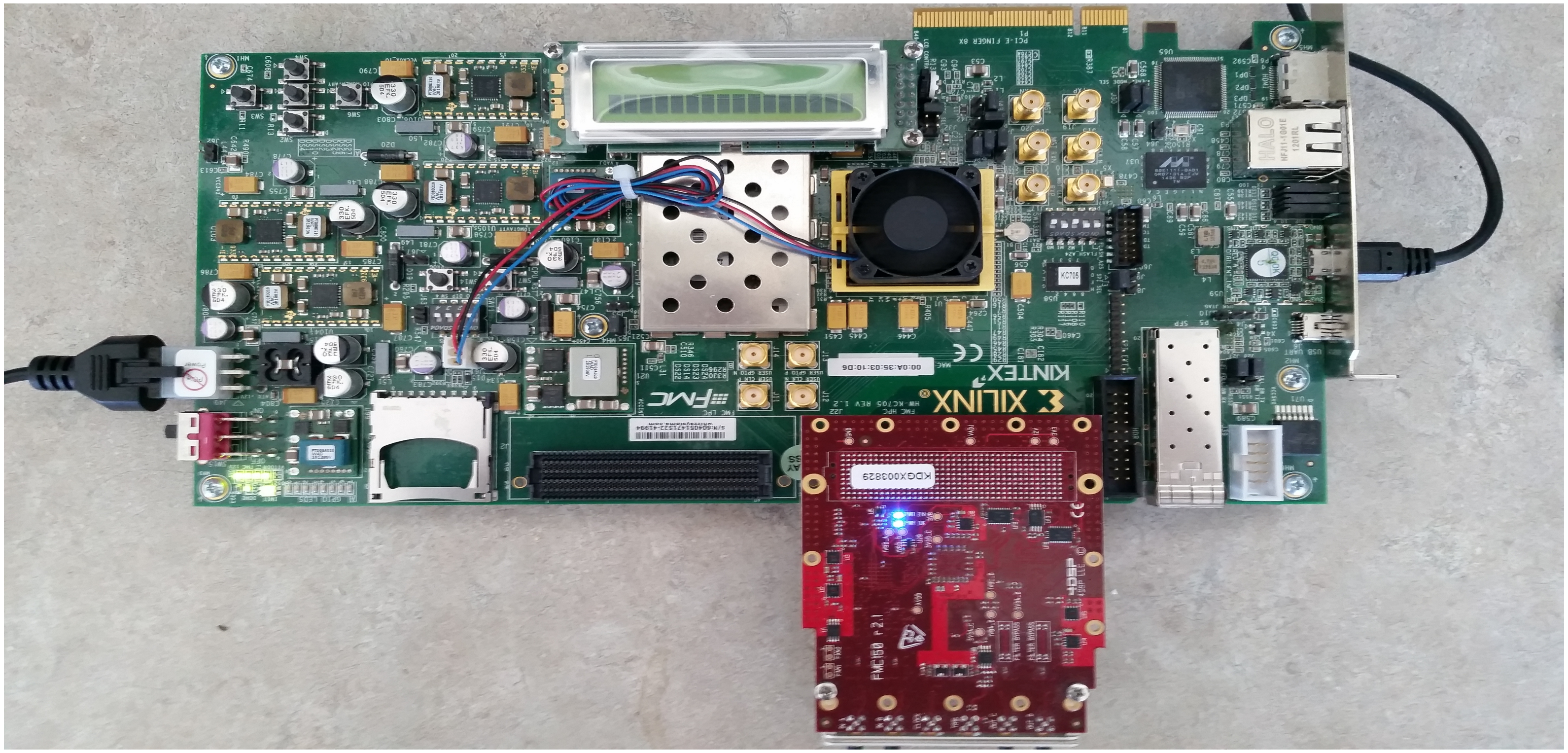

Figure 3.2. Kintex 7 FPGA Development Kit with Digital Signal Processing (DSP) Daughter Card.

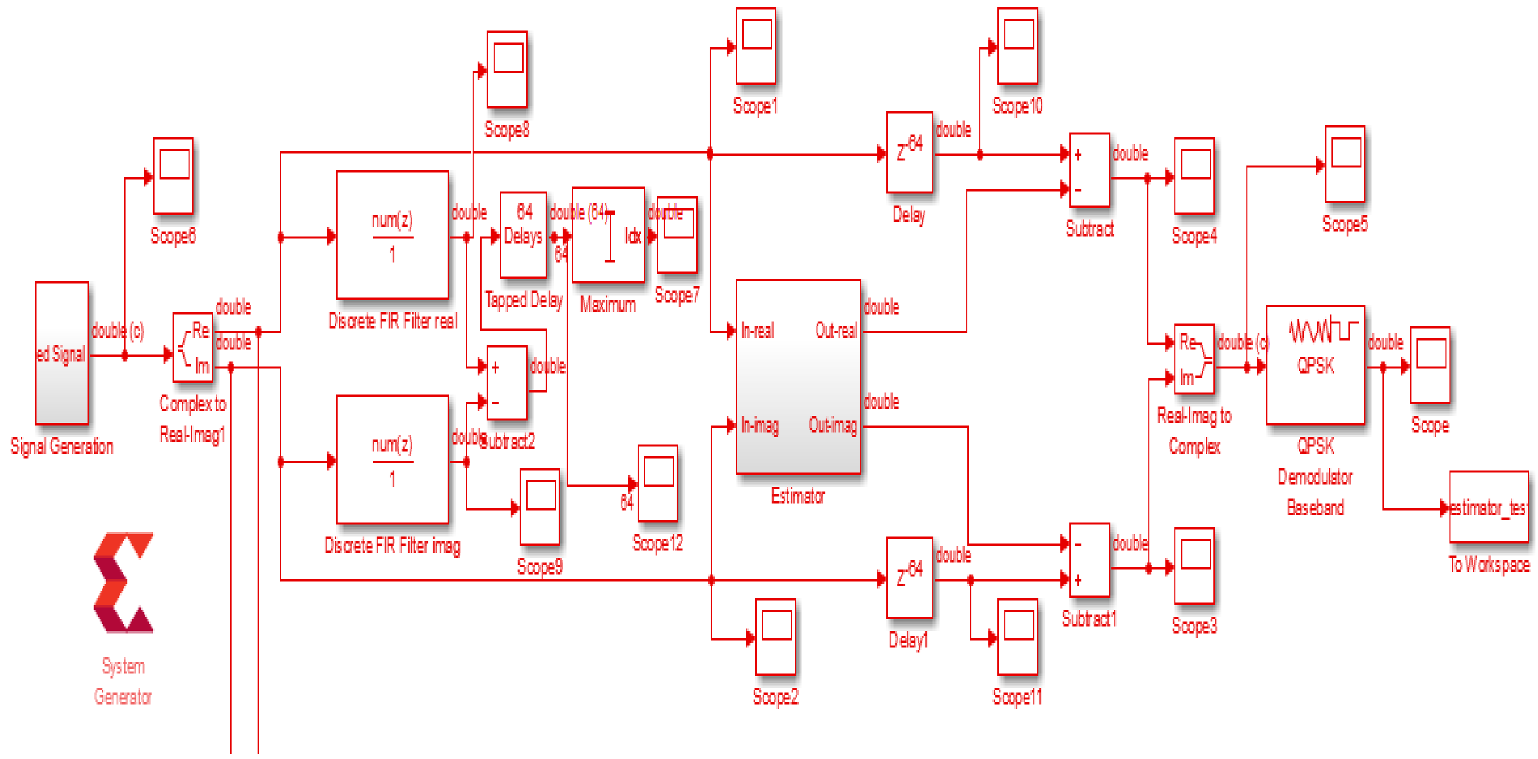

Figure 3.3. Simulink P_D with Signal Duration Estimation.

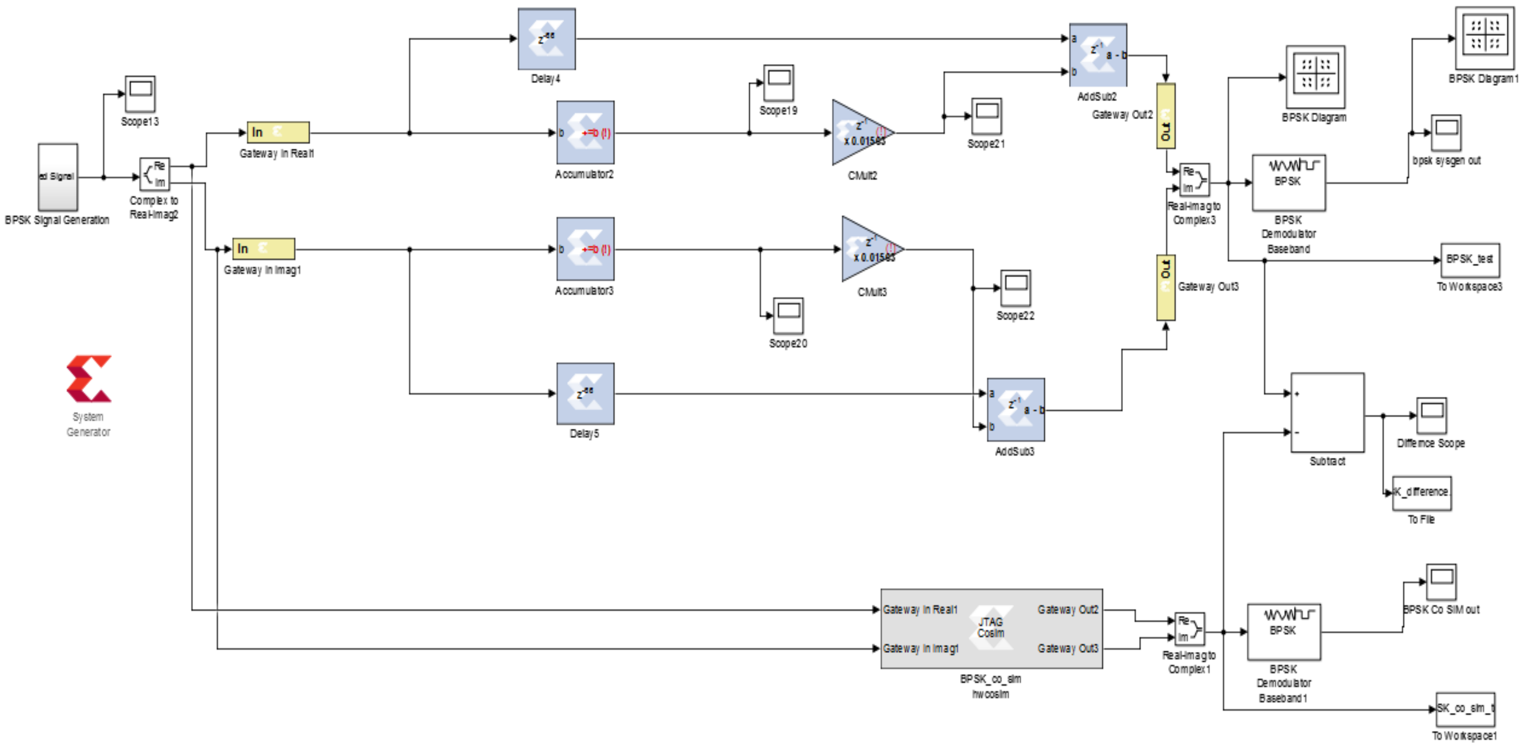

Figure 3.4. Simulink and FPGA BPSK Model Showing the Signal Estimation and Communications Demodulation.

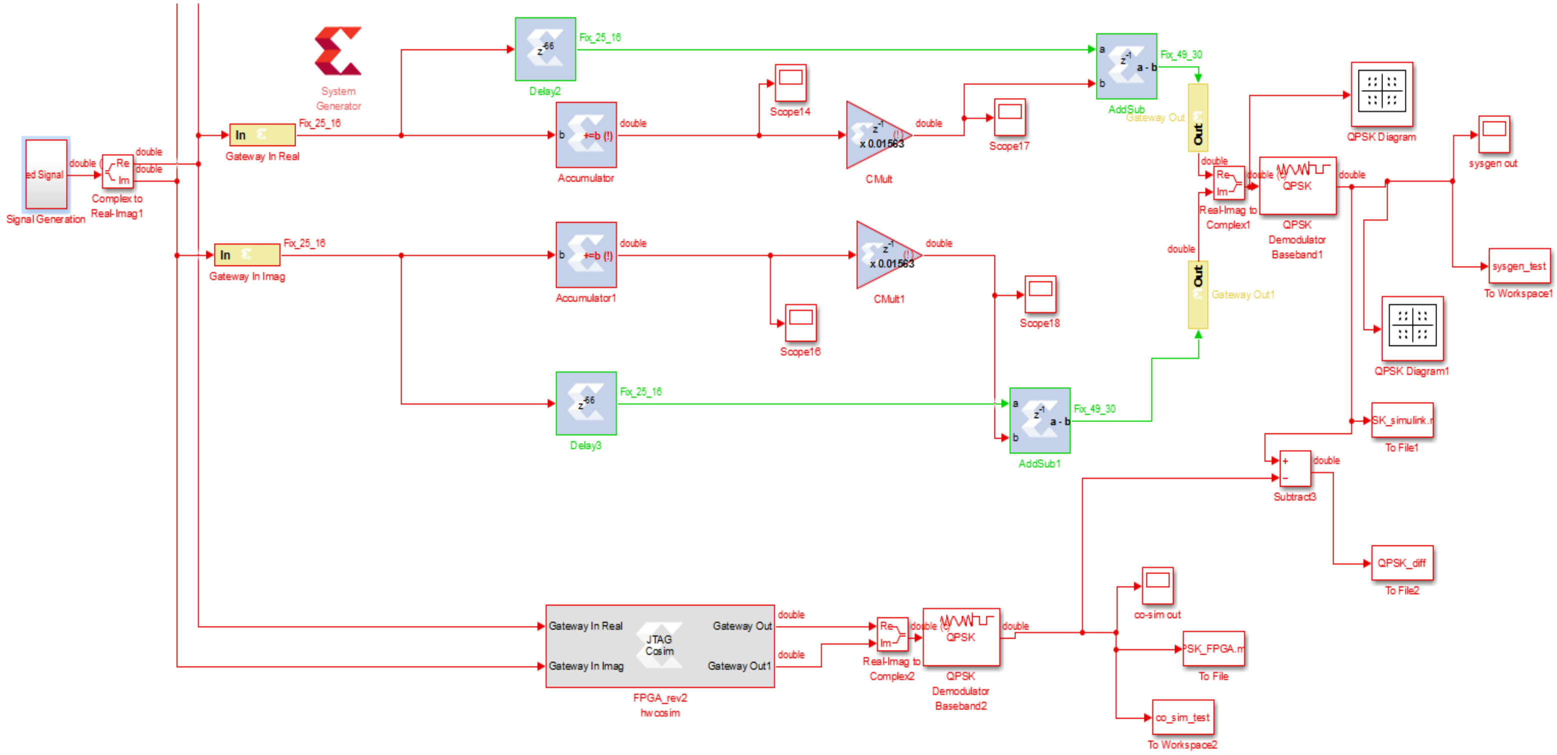

Figure 3.5. Simulink and FPGA QPSK Model Showing the Signal Estimation and Communications Demodulation.

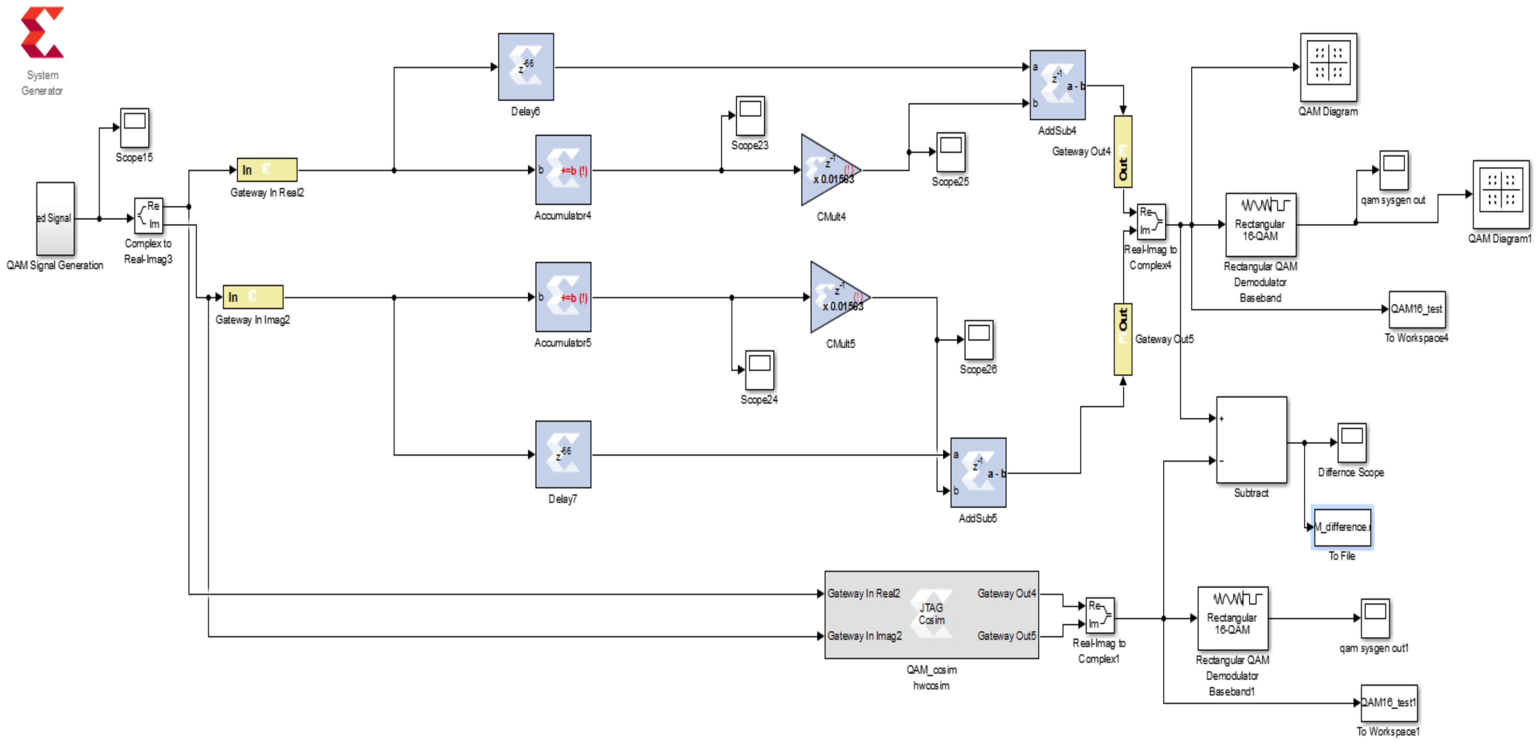

Figure 3.6. Simulink and FPGA 16QAM Model Showing the Signal Estimation and Communications Demodulating.

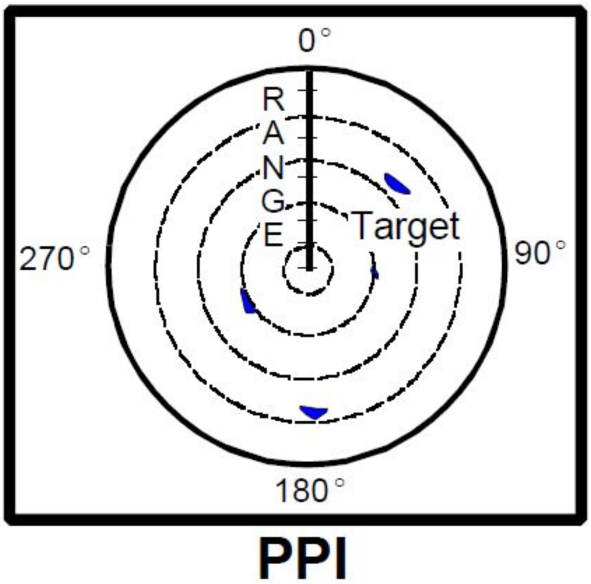

Figure 3.7. Graphical Depiction of the PPI Scope of a Radar. Source: [16].

that the communications signal is low-powered compared to the radar signal.

3.5.1 Plan Position Indicator

In this section, we see if a radar operator looking at the PPI display is able to determine the presence of a communications signal co-channel with the radar. This common radar display depicts the radar pulse return in polar coordinates as a function of range and bearing. The video displayed post signal processing is usually from an energy detector [15] as shown in Figure 3.7.

We then attempt to construct a virtual terrain and display it on the PPI. We qualitatively conclude if a signal is covert or not if it can be separated from the terrain.

3.5.2 Exploring the Complex Plane

In this section, we consider a situation where a non-cooperative receiver (STA-3) eavesdrops on the conversation between STA-1 and STA-2. This scenario is illustrated in Figure 3.8. We examine the complex plane of the signal observed at STA-3. We see if the communications signal is discernable by considering the in-phase and quadrature (I/Q) components of the signal. If the communications signal within the radar signal is to remain covert, we prefer the appearance of random points within the complex plane to be centered around the position of the radar pulse. We note that the noise power at the receiver is different at STA-2 and STA-3 due to differences in receiver sensitivities driven by differing bandwidth requirements. The signal power at each station is also different because of the different path lengths and effects between STA-2 and STA-3. We note that STA-3 could be receiving the signal via STA-1 antenna's sidelobe, reducing signal power. All of these effects indicate that there will be a difference in C-SNR between STA-2 and STA-3. Due to position and sidelobe reception, STA-3 will most likely operate at a disadvantage as is standard in classical LPI scenarios. In Figure 3.9, we show an arbitrary radar pulse without communications embedding. The signal was sent with a phase of $\pi/4$ and a SNR of 30 dB. The amplitude of each open blue circle is a discrete sample of the radar pulse and is distorted by noise from the ideal. The radar phase actually rotates through the complex plane as it travels to reach a receiver and will be a fixed but unknown quantity which must be estimated. In the complex plane, the appearance of a deterministic structure centered around the radar's phase plot estimate may indicate embedded data. The signal changes phase as the distance between the transmitter and receiver changes and the carrier signal changes phase. If the data is QPSK, the complex plane without noise is shown in Figure 3.10. Using the subtraction method discussed in Section 3.2, we can remove an estimate of the radar signal from the received signal, as in Equation (3.6). By removing the radar estimate, any remaining structure of the signal may be observable. Through estimation and subtraction, the complex plane for each of the various data embedded radar signals is centered around the origin.

In the next chapter, we examine the results of these detection and demodulation techniques.

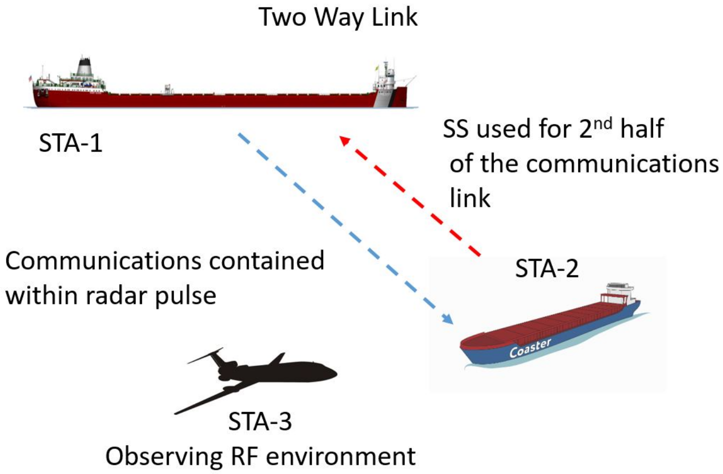
Two Way Link
STA-1
SS used for 2nd half of the communications link
Communications contained within radar pulse
STA-2
Coaster
STA-3
Observing RF environment

Figure 3.8. A Scenario with an Uncooperative Receiver Eavesdropping on the Conversation Depicted in Figure 1.4.

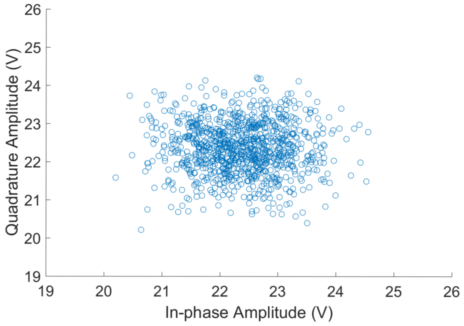

Figure 3.9. Graphical Depiction of a Constant Phase Radar Signal in the Presence of Noise.

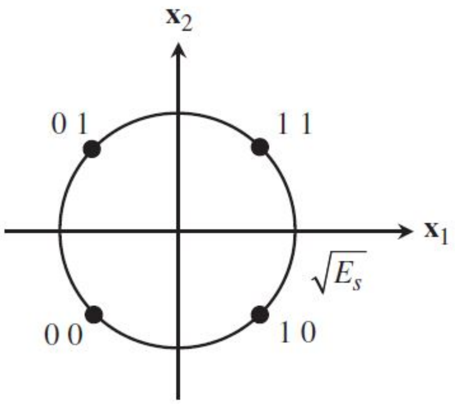

Figure 3.10. Graphical Depiction of In-phase and Quadrature Axes for a QPSK Signal. Source: [17].

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Results

In this chapter, we explore the findings of our work. We first quantify our P_D results. We then follow this with our simulated SER for the modulation schemes outlined in Section 2.2. We next examine the results of our hardware co-simulation. Finally, we close this chapter with qualitative results on the covertness of the communications within the radar-data signals.

4.1 Probability of Detection

When using matched filter detection matched to the radar pulse only, an embedded communications signal as proposed in [5] and [6] degrades the probability of detection as shown in [4]. In this work, we embed the communications signal in the transmitted pulse and can, therefore, coherently detect the radar return with the unique waveform sent. The additional energy included in the transmitted waveform eliminates the P_D degradation and now serves to increase the P_D. This effect is seen most at lower RCRs. In this section, we compare three P_D curves for various RCRs. The P_D curves from the theoretical expression for radar-pulse-only are shown as the solid blue lines in the ensuing figures. The P_D curves resulting from the radar-pulse-only matched filter on the radar-communications signal are shown as the dashed red lines. Finally, the P_D curves for radar-communications matched filter detection are shown as the solid black lines.

The P_D comparison is most easily seen in Figure 4.1, where the detection curve for a communications embedded pulse using radar-pulse-only filter is slightly degraded compared to the theoretical P_D curve for radar-only signal except for low SNR. In this case, notice that the radar and communications signals have equal energy; i.e., RCR = 0 dB and the SRBR = 4. We realize approximately 3 dB of gain over the theoretical P_D through matched-filtered detection of the communications-radar signal. Across all SNRs, the communications-radar matched filtered case shows increased P_D over the theoretical curve due to the increased energy and matched-filtering.

It is unlikely that the signal will be sent with RCR = 0 dB as shown in Figure 4.1, as that negates our LPI assumption. For the assumption in Equation (3.4), the communications-

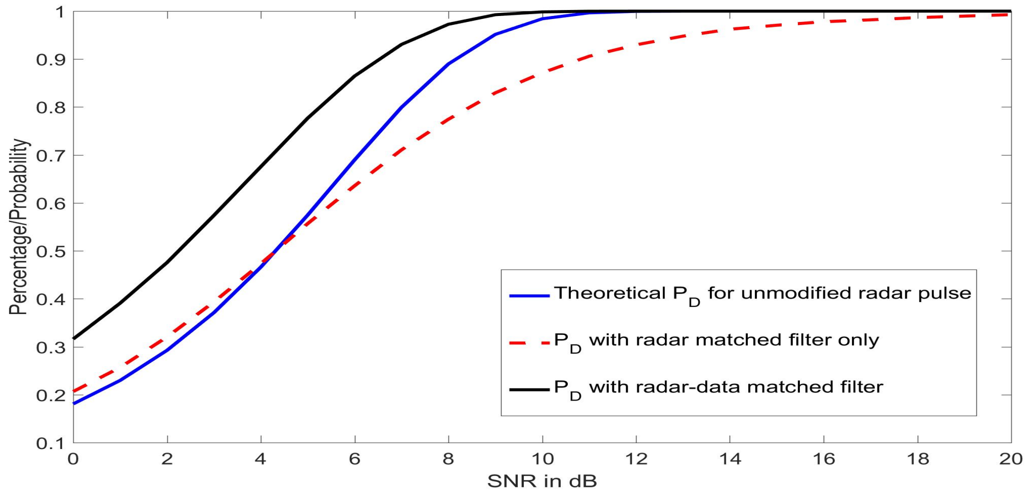

Figure 4.1. Comparison of Theoretical, Radar-Pulse-Only Matched Filter, and the Radar-Communications Matched Filtered P_D Curves versus SNR for RCR = 0 dB.

radar signal will be sent with higher RCRs. In Figure 4.2, we present the theoretical P_D for the radar-only signal (blue line), P_D using radar-only matched filter (dashed red line), and the P_D of matched filter to combined radar-data signal (solid black line) for the cases of RCR = [3, 6, 10] dB with a SRBR of 4. A few observations are seen in Figure 4.2. First, P_D for communications-radar pulse matched filtered detection is always greater than the theoretical P_D for radar-pulse-only signal and the P_D for the radar-only matched filter. Second, as RCR increases, the P_D advantage decreases. Finally, as RCR increases, the P_D of both the radar-only matched filtered case and the radar-communications matched filtered case appear to converge to the theoretical P_D. As less communications energy is added to the pulse, the P_D of the embedded communications-radar pulse decreases but is clearly better than the other two curves.

4.2 Symbol Error Ratio

The metric for the embedded communications performance is SER. To produce SER results, we perform Monte Carlo (MC) simulations by tracking the number of symbol errors divided by the total number of symbols sent. We track the errors for each particular SNR to determine the SER at that SNR. We perform 10^5 or 10^6 MC trials for each communications signal-to-

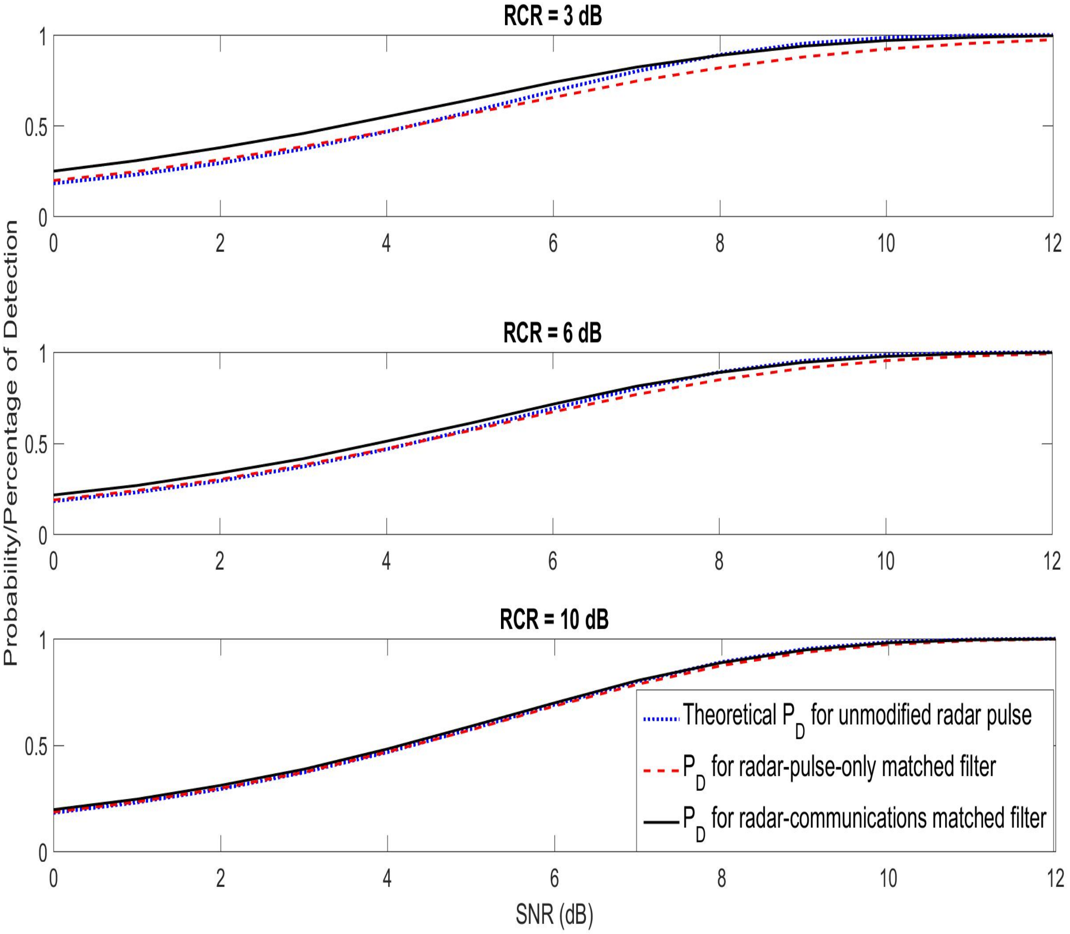

Figure 4.2. Comparison of Theoretical, Radar-Pulse-Only Matched Filter, and the Radar-Communications Matched Filtered P_D Curves versus SNR for RCR = [3, 6, 10] dB.

noise ratio (C-SNR). The choice between 10^5 or 10^6 MC trials is based off producing smooth SER curves. Here, we initially simulate the case where we make no attempt to estimate the radar signal parameters (N=0). Then we simulate the cases where N = [8, 16, 32, 64, 128, full signal length]. In our simulations, "N = full signal length" corresponds to using each discrete sample of the signal. For modified 8PSK and 16QAM, full signal length is 300 samples. BPSK's full signal length is 30,000. QPSK's and 8PSK's full signal length is 10,000. In all cases, when there is no attempt to estimate the radar parameters and subtract

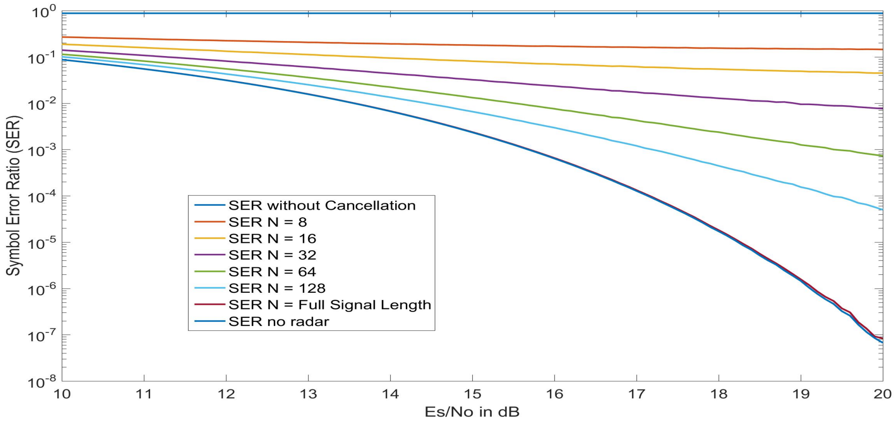

Figure 4.3. SER Performance of BPSK as a Function of the Size of the Estimator (N).

it from the received signal prior to demodulation, notice that the SER is unacceptably poor. We also notice that as N increases, we obtain a better radar estimate, and SER decreases for all modulations under test. This result is consistent with theory [18]. In order to compare a communications-only channel to the radar-embedded communications channel, we include a "SER no radar" curve, where "SER no radar" is the SER curve for the communications-only channel.

4.2.1 BPSK

The SER curves for BPSK are shown in Figure 4.3 with $3 \cdot 10^{10}$ samples per SNR. Using 10^{6} MC trials, we show the SER curves for the differing estimator sizes (N = 0, 8, 16, 32, 64, 128, and 30,000). As N increases, SER improves as expected. The N = 10,000, or full-signal length case, is only slightly worse than the communications-only channel, and the results for these cases are very similar. Indeed the two curves lie on top of one another in Figure 4.3.

4.2.2 QPSK

Our results for QPSK verify the work of [3]–[6]. We conducted 10^{5} MC trials, of 10^{9} samples per SNR with results shown in Figure 4.4. All of the SER curves decrease with increasing C-SNR, as expected. For the QPSK modulation, the full-signal length was $10,000$ symbols. The full-signal length case is only slightly worse than the communications-only

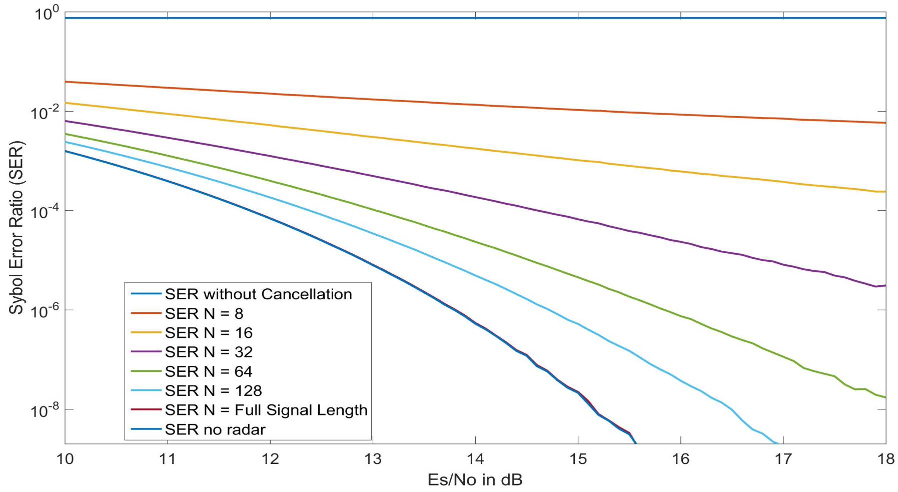

Figure 4.4. SER Performance of QPSK as a Function of the Size of the Estimator (N).

channel and the results for these cases are very similar. Indeed, the two curves lie on top of one another in Figure 4.4.

4.2.3 8PSK

For 8PSK, we again utilized 10^5 MC trials, with 10^9 samples per SNR and results shown in Figure 4.5. The results are consistent with our general findings of PSK signals; as N increases, the SER decreases. For the 8PSK modulation, the full-signal length was $10,000$ symbols.

4.2.4 Modified 8PSK

For the modified 8PSK, we utilized 10^6 MC trials, with $3 \cdot 10^8$ samples per SNR. The modified 8PSK has a degraded SER compared to ideal 8PSK as expected, even with increasing estimator sizes. The degraded SERs are shown in Figure 4.6. This is due to the closeness of the symbols in the complex plane. For very large N, the resulting SER approaches the theoretical SER of modified 8PSK only (as is the case where the radar power is zero). For the modified 8PSK modulation, a full-signal length of 300 symbols was used.

This type of modulation is an option in the trade space of SER and LPI. If only modest SER is required, then this modulation may be acceptable. If decreased SER is needed,

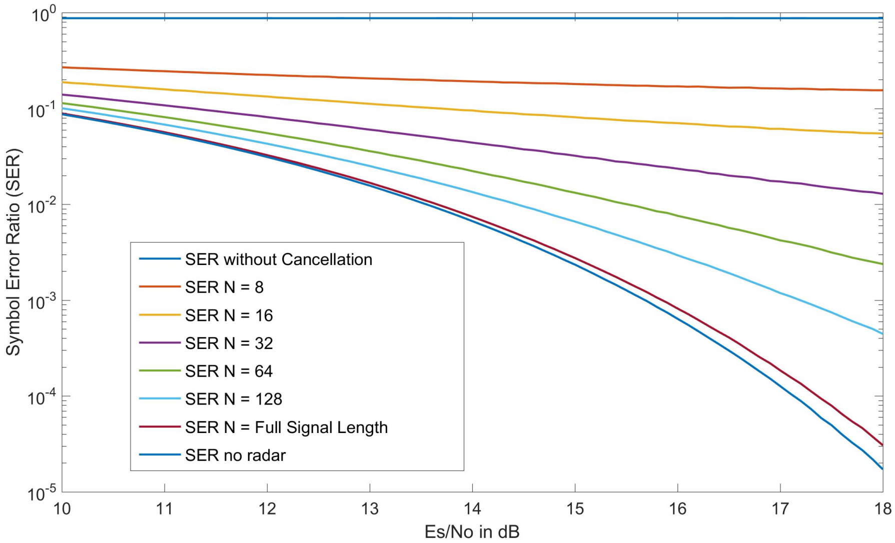

Figure 4.5. SER Performance of 8PSK as a Function of the Size of the Estimator (N).

then further separation of symbols in the constellation plane is required or forward error correction may be implemented.

4.2.5 16QAM

We utilized 10^6 MC trials for 16QAM with $3 \cdot 10^8$ samples per SNR. The SER curves are shown in Figure 4.7, where as N increases, SER decreases. Also shown in Figure 4.7, as with all the other SER curves, as C-SNR increases, SER decreases. For the modified 16QAM modulation, the full-signal length was 300 symbols.

4.3 Hardware Results

Using the models shown in Section 3.4, we demodulated BPSK, QPSK, and 16QAM signals. The results of hardware co-simulation show that the Simulink model and FPGA model produce the same results. For each of these three modulations, 64 symbols were sent with RCR = 20 dB and C-SNR = 10 dB.

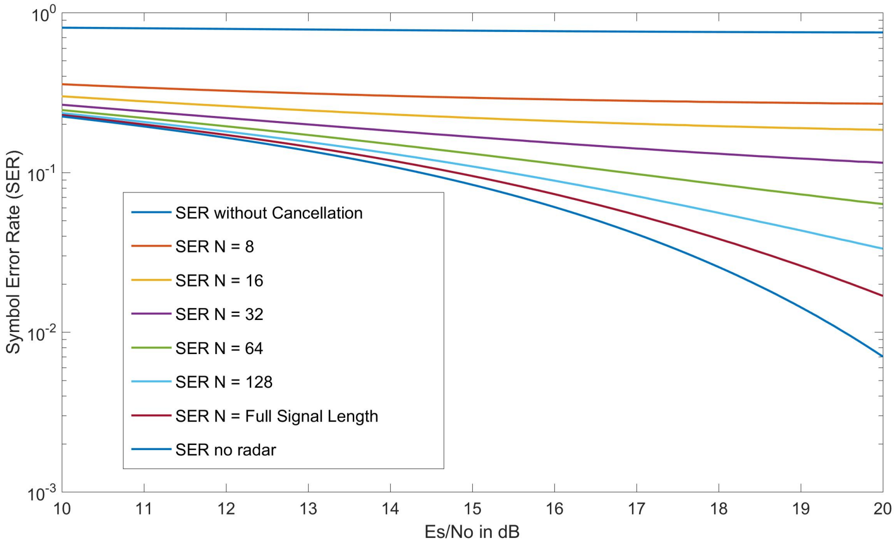

Figure 4.6. SER Performance of Modified 8PSK as a Function of the Size of the Estimator (N).

4.3.1 FPGA Model performance

For the 64 symbols sent within the PRIs tested, there is no measurable difference in output between implementation methods. This gives greater confidence to our software models.

Due to time constraints, we were unable to implement communications estimation and demodulation synchronized off the detection of the embedded radar pulse. Because we were unable to trigger demodulation following detection, we did not attempt MC trials to determine FPGA SERs.

With a difference of exactly zero between the FPGA and software model outputs, we choose the Simulink output to display our results. In Figure 4.8, we see the output of the BPSK demodulator. The demodulator converts the complex plane representation of the symbol to the symbol number. We can easily see where the signal is temporally located within the trace. The value shown on the y-axis is the demodulated symbol, either a 0 or a 1. The x-axis shows the normalized sampling time T_S. The flat lines show the portion of time when no signal is present. The rapid change seen around $t = 64$ is the change from one symbol to another. We can see the QPSK demodulated signal in Figure 4.9. Again, we can see where the signal is located in time within the trace. Only one symbol is sent during each sample,

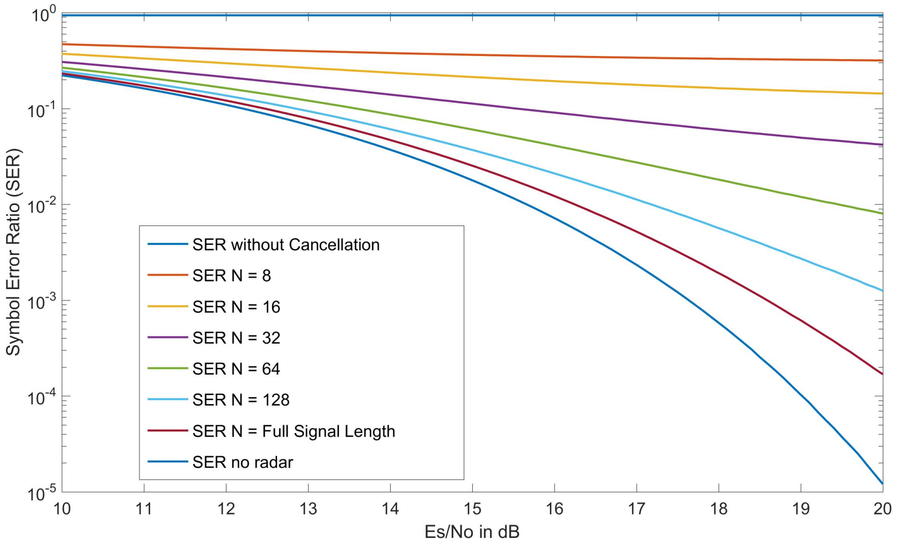

Figure 4.7. SER Performance of Modified 16QAM as a Function of the Size of the Estimator (N).

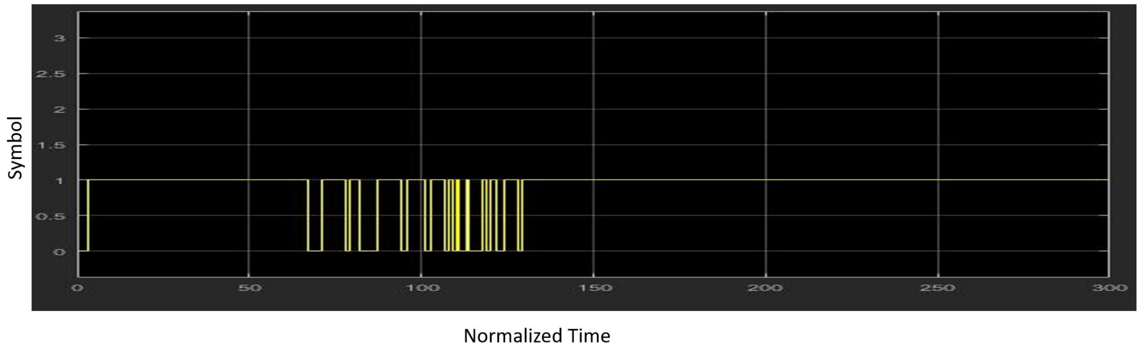

Figure 4.8. The BPSK Simulink and FPGA Waveforms over Time.

and the value of the demodulated symbol (0, 1, 2, or 3) is shown on the y-axis. Finally, in Figure 4.10 we see output of the 16QAM demodulator. We again see where the data signal is located within the trace. While we were unable to trigger the estimation process through pulse detection, we have shown that symbols can be received and processed in a FPGA.

4.4 Covertness Analysis

We now turn our attention to the qualitative measure of the concealment of the data within the radar pulse. First we examine the PPI display available to the radar operator. Then we

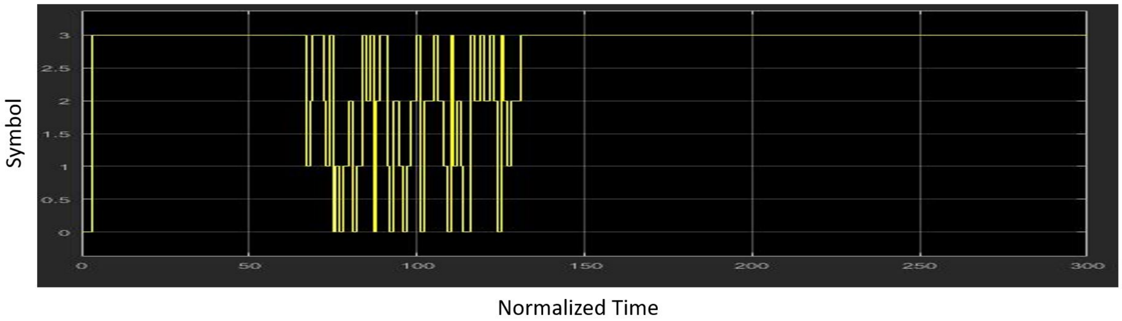

Figure 4.9. The QPSK Simulink and FPGA Waveforms over Time.

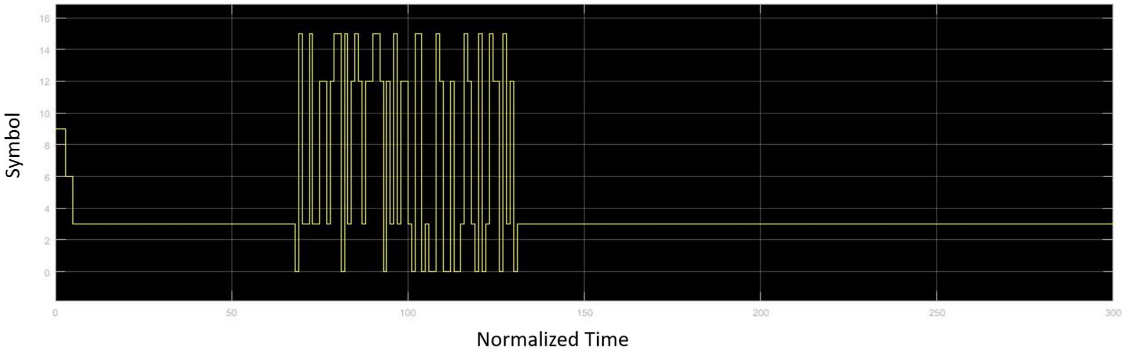

Figure 4.10. The 16QAM Simulink and FPGA Waveforms over Time.

explore the complex plane maps of the embedded pulse following the estimator. For this section, we maintained an RCR of 20 dB.

4.4.1 Plan Position Indicator Display

For this qualitative result, we look at two figures of the same simulated terrain. The terrain is shown in yellow, while the sea is shown in blue. The display is typical of what is seen on the radar scope while operating near a coastline. Any "yellow" pixels seen in the blue "water" are due to noise in our simulations. These false detections appear with a predictable regularity based on the chosen PFA of the simulation. While many simulations were conducted, the results differed little. Communications symbols were embedded within the radar signal used to produce the PPI display seen in Figure 4.11. Communications symbols were not embedded within the radar signal used to produce the PPI display shown in Figure 4.12. When presented with these two images, it is unlikely one would notice the effects of the change in waveform.

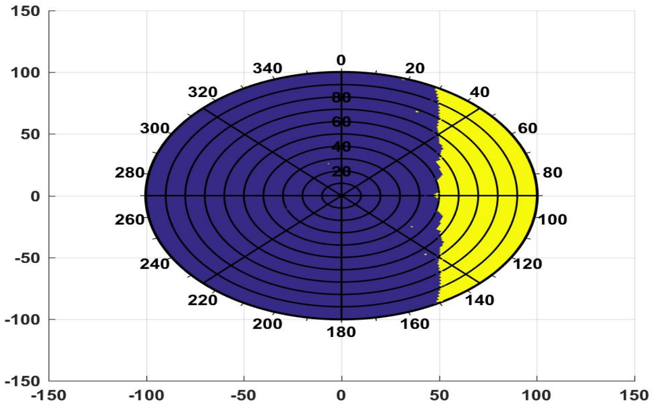

Figure 4.11. View of the PPI Display Available to a Radar Operator Viewing Embedded Covert Communications.

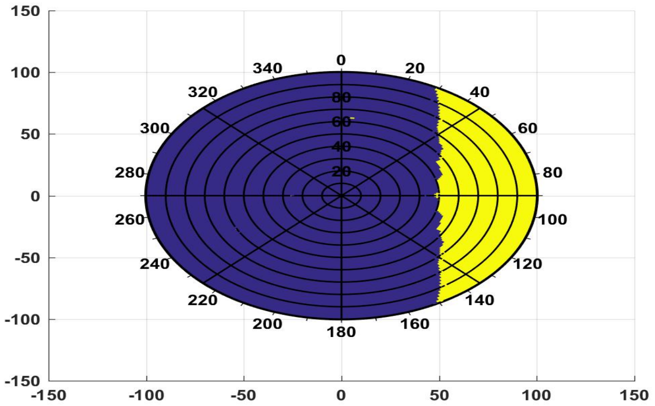

Figure 4.12. View of the PPI Display Available to a Radar Operator Viewing a Radar Signal with No Embedded Communications.

4.4.2 LPI Analysis via Complex Plane Mapping

We now turn to the complex plane of the communications-radar signal. Recall that in this case, we consider the case where the eavesdropper (STA-3) listens to the STA-1 to STA-2 conversation. We qualitatively observe embedded information and see if we identify regularities within the complex plane. Because we were only testing the covertness of each modulation scheme and were not interested in real-time demodulation, we used the largest estimator size N available. As discussed in Section 3.5.2, we note that since STA-3 is the eavesdropper, its SNR is most likely worse than STA-2. But if its sensitivity approaches that

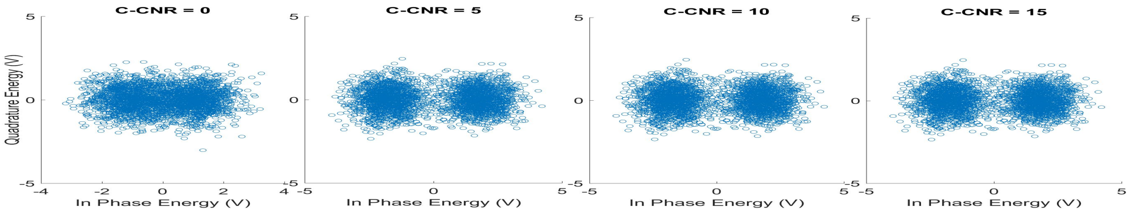

Figure 4.13. The Complex Plane View after Estimator Subtraction of BPSK Signal for C-SNR = [0, 5, 10, 15] dB.

of the intended receiver, its SNR increases. As the SNR increases, the embedding is more obvious. We maintain a RCR of 20 dB for the results presented in this section. With the notable exception of the modified 8PSK, all the signals appear as expected in the complex plane.

BPSK

Depictions of 1000 random BPSK symbols for each C-SNR 0, 5, 10, and 15 dB are shown in Figure 4.13. The BPSK embedded signal at C-SNR = 0 dB appears as if the radar signal is subject to random noise. If the eavesdropper is indeed at a disadvantage, then a C-SNR = 0 dB (at its receiver) is a good covert case from the perspective of the intended receiver; however, as the C-SNR increases, the symbols become more distinct. Even at C-SNR as low as 5 dB, two separate clusters can be seen.

QPSK

Depictions of 1000 random QPSK symbols for each C-SNR 0, 5, 10, and 15 dB are shown in Figure 4.14. The QPSK embedded signal at C-SNR = 0 dB appears as if the radar signal is subject only to random noise; however, as the C-SNR increases, more order appears within the signal. At C-SNR = 5 dB, we can discern edges in the complex plane. By C-SNR = 10 dB the clusters expected for a QPSK signal are unmistakable. The large C-SNR case implies a receiver comparable to that of the intended receiver.

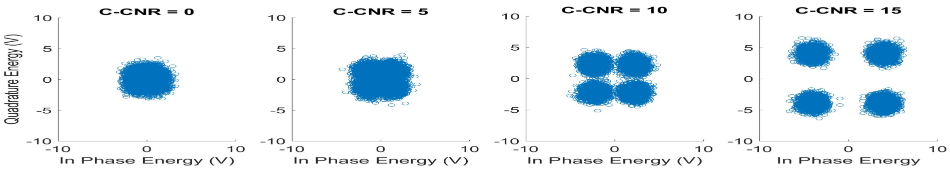

Figure 4.14. The Complex Plane View after Estimator Subtraction of QPSK Signal for C-SNR = [0, 5, 10, 15] dB.

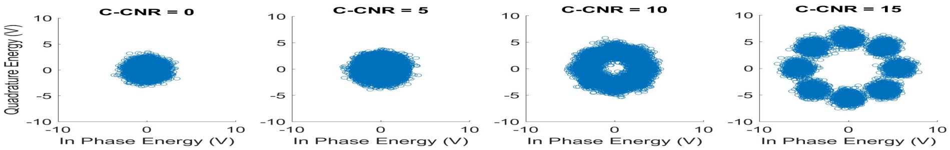

Figure 4.15. The Complex Plane View after Estimator Subtraction of 8PSK Signal for C-SNR = [0, 5, 10, 15] dB.

8PSK

Depictions of 1000 random 8PSK symbols for each C-SNR 0, 5, 10, and 15 dB are shown in Figure 4.15. The 8PSK embedded signal at C-SNR of 0 dB and 5 dB appears as if the radar signal is subject to only random noise; however, as the C-SNR increases, the phases of the become more distinct. At C-SNR = 10 dB we can distinguish a clear annulus, with the eight distinct phases visible at C-SNR = 15 dB.

Modified 8PSK

Depictions of 1000 random modified 8PSK symbols for each C-SNR 0, 5, 10, and 15 dB are shown in Figure 4.16. The modified 8PSK embedded signal at C-SNR = 0 dB appears as if the radar signal is subject only to random noise; however, as the C-SNR increases, more order appears within the system. At C-SNR = 5 dB, we can discern edges in the complex plane. By C-SNR = 15 dB, the clusters we expect for a QPSK signal are unmistakable. Even when this modified signal is found, it appears as QPSK. This adds another layer of covertness and increases the LPI quality of this signal. When viewing this signal in the

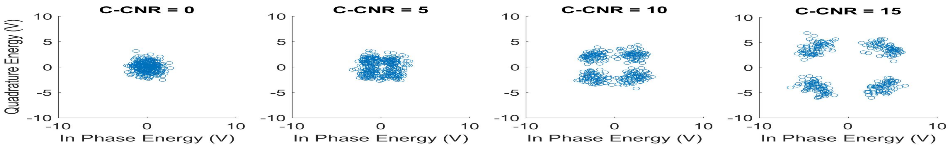

Figure 4.16. The Complex Plane View after Estimator Subtraction of Modified 8PSK Signal for C-SNR = [0, 5, 10, 15] dB.

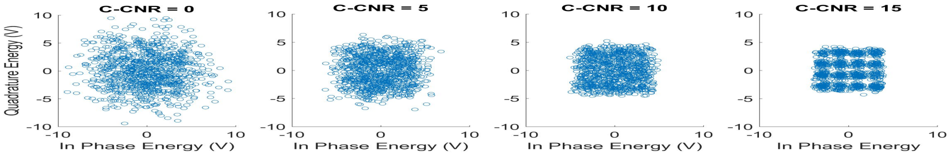

Figure 4.17. The Complex Plane View after Estimator Subtraction of 16QAM Signal for C-SNR = [0, 5, 10, 15] dB.

complex plane, STA-3 would likely confuse it with QPSK. Any attempted demodulation of modified 8PSK with a QPSK algorithm will produce excessive errors.

16QAM

Depictions of 1000 random 16QAM symbols for each C-SNR 0, 5, 10, and 15 dB are shown in Figure 4.17. The 16QAM embedded signal at C-SNR = 0 dB appears as if the radar signal is subject only to random noise; however, as the C-SNR increases, more order appears within the signal. At C-SNR = 5 dB, we can discern edges in the complex plane. At C-SNR = 10 dB, the received signal appears as a box. By C-SNR = 15 dB, the clusters we would expect for a 16QAM signal are unmistakable.

Qualitatively covertness was lost when the C-SNR at STA-3 is 5 dB for all modulations studied except 8PSK. The 8PSK modulation appeared covert until C-SNR reached 10 dB. The modified 8PSK loses some of its covertness for C-SNR ≥ 5 dB; however, it masquerades as a QPSK signal.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5: Conclusions and Future Work

In this chapter, we conclude our work and indicate future opportunities for research in this exciting field.

5.1 Conclusions

In this work, we proposed a half-duplex data link with the use of radar-embedded communications and direct sequence spread spectrum. We concentrated on the design of the downlink by embedding data into the radar pulse. With radar-data matched filter detection, we showed an increase in P_D compared to radar-pulse-only matched filter detection. We showed that a downlink channel can be designed while simultaneously improving radar P_D performance. We verified that modulation schemes other than QPSK are possible to demodulate even when embedded in a 20 dB stronger radar pulse. Specifically, the technique was shown to work with both amplitude and phase modulated signals. Rigorous SER requirements can be met when using BPSK. The 8PSK modulation scheme provided high data rates with good SER. The modified 8PSK (designed for LPI considerations) was possible to demodulate, although the symbols were too closely spaced for stringent SER. The 16QAM showed the possibility of high data rates with good SER. Finally, we analyzed covertness in the complex plane (as parameterized by SNR in a non-cooperative receiver). We showed, in the classic LPI eavesdropping scenario, C-SNR at STA-3's receiver must have a SNR of 0 dB for the communications to be covert and be less than 5 dB to preserve some degree of covertness. When the embedded signal is viewed on a PPI display, it was difficult to discriminate it from a non-embedded signal. We found as the C-SNR increased at an eavesdropping receiver, the covertness of the signal decreased when viewed through the complex plane.

5.2 Future Work

We believe there are four areas of this thesis that could use further research. First, investigate taking a transmitted radar-communications signal and transitioning the true RF signal into data messages on the EEMS laboratory network. This requires working hardware detection and demodulation to encapsulate the data into the appropriate network protocols for maritime network transmission. Second, we recommend further research into the estimator size. The size of the estimator needed depends on a particular application and is coupled with the SER and real-time requirements needed by that particular application. A specific case study should be explored considering the maritime network that a radar communicates to (specifically in the EEMS laboratory). The study of the estimator size should focus on hardware constraints and reducing signal processing delay caused by an over-sized estimator. This should also include how much of the communication-radar signal should be used in the estimator, how many symbols to embed, and in what portion of the pulse the symbols should be embedded (beginning, middle, end). This ties in nicely with the requirement for data rate analysis for that particular case study mentioned above. Finally, we recommend further investigation into analysis of the embedded communications as a covert signal using quantitative metrics such as probability of intercept as opposed to the qualitative analysis performed in this work.

List of References

[1] IMO profile overview, 2017. URL https://business.un.org/en/entities/13. Accessed Oct. 7, 2017.

[2] US DHS: United States Coast Guard. *Navigation Rules: International - Inland*. Paradise Cay Publications, Arcada, CA, 2004.

[3] G. Meager. High powered radar interference estimation and cancellation for weak signal collection and demodulation. M.S.EE thesis, Department of Electrical and Computer Engineering, Naval Postgraduate School, Monterey, CA, 2017.

[4] A. Hunt. Various effects of embedded intrapulse communications on pulsed radar. M.S.EE thesis, Department of Electrical and Computer Engineering, Naval Postgraduate School, Monterey, CA, 2017.

[5] G. Meager, R. A. Romero, and Z. Staples. "Estimation and cancellation of high powered radar interference for communication signal collection". In *2016 IEEE Radar Conference (RadarConf)*, pages 1–4, May 2016. doi: 10.1109/RADAR.2016.7485263.

[6] T. W. Tedesso, R. Romero, and Z. Staples. "Analysis of a covert communication method utilizing non-coherent dpsk masked by pulsed radar interference". In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2082–2086, March 2017. doi: 10.1109/ICASSP.2017.7952523.

[7] Z. Staples. EEMS CCW Brief. Unpublished.

[8] Does VSAT have a role in IoT, 2015. Available: https://www.slideshare.net/iDirect/does-vsat-have-a-role-in-iot-58400349. Accessed Oct. 7, 2017.

[9] M. Wingrove. Ships are already under cyber attack. Marine: Electronics and Communications. [Online]. April 2017. Available: http://www.marinemec.com/news/view,ships-are-already-under-cyber-attack_47344.htm.

[10] C. Baraniuk. How hackers are targeting the shipping industry. BBC News. [Online]. August 2017. Available: http://www.bbc.com/news/technology-40685821.

[11] Shannon D. Blunt and Casey R. Biggs. Practical considerations for intra-pulse radar-embedded communications. In *International Waveform Diversity and Design Conference*, pages 244–248, Kissimmee, FL, February 2009.

[12] Kevin D. Shepherd and Ric A. Romero. Radar waveform design in active communications channel. In *Asilomar Conference on Signals, Systems and Computers*, pages 1515–1519, Pacific Grove, CA, November 2013.

[13] Merrill L. Skolnik. *Introduction to RADAR Systems, 3rd Ed.* McGraw Hill, New York, NY, 2001.

[14] Steven M. Kay. *Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory*. Prentice Hall, Upper Saddle River, NJ, 1993.

[15] Operator's guide to marine radar. Available: https://www.furunousa.com/Learning%20Center%20Documents/FurunoRadarGuide-LR.pdf. Accessed May 10, 2017.

[16] *Electronic Warfare and Radar Systems Engineering Handbook*. Naval Air Warfare Center - Weapons Division, 2012.

[17] Tri T. Ha. *Theory and Design of Digital Communication Systems*, chapter 6. Cambridge University Press, Cambridge, UK, 2011.

[18] Charles W Therrien. *Probability and random processes for electrical and computer engineers*. CRC Press, Boca Raton, FL, 2nd edition.

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California